Task: BentoboxV1 Assesment Audit
Goal: To find a vulnerability that can lead to loss of funds
Assigned to: Darshan Jogi
Email: Darshanbughunter@gmail.com

Findings:

Title: Flash Loan Vulnerability

Summary

BentoboxV1 smart contract is vulnerable to a logical vulnerability in its flash loan repayment mechanism. Specifically, the contract uses its balance to determine if the flash loan has been repaid.

Vulnerability Details

contract checks if the balance meets or exceeds the total amount required, but it does not verify the source or intent of the balance increase.

Steps To Reproduce Attack-

1. The attacker writes a malicious contract that takes out a flash loan for the maximum possible amount.
2. The attacker ensures the borrowed amount includes the required fees.
3. Instead of repaying the flash loan directly, the attacker deposits the total borrowed amount (including fees) into the BentoBox contract.
4. The contract incorrectly registers the flash loan as repaid due to the increased balance. as function _tokenBalanceOf relies on token.balanceOf(address(this).

```

 require(_tokenBalanceOf(token) >= totals[token].addElastic(fee.to128()), "BentoBox: Wrong amount");

```

```
function _tokenBalanceOf(IERC20 token) internal view returns (uint256 amount) {
        amount = token.balanceOf(address(this)).add(strategyData[token].balance);
    }

```

5. .The attacker withdraws the deposited funds, draining the BentoBox contract.

Impact

Loss of funds

Recommendations

Introduce a separate tracking mechanism to ensure flash loan repayments originate from the borrower.